Navy Marine Corps Intranet Security

NMCI Program

The Navy Marine Corps Internet (NMCI) is a long term arrangement between the Department of the Navy (DON) and the private sector to deliver comprehensive, end-to-end information services including capital infrastructure improvements, maintenance, training and operation of the full spectrum information technology required by our Naval and Marine Corps warfighters. The scope of this effort includes everything necessary to ensure the secure transmission of voice, video and data information between authorized users within the Continental United States (CONUS), Hawaii, Guantanamo Bay (Cuba), Puerto Rico and Iceland.

With the significant benefits of increasing network connectivity comes a corresponding increase in the potential for detrimental information warfare (IW) attacks and physical threats from natural and man-made disasters. As modern warfare becomes more dependent on information technology (IT) resources like NMCI services, NMCI network defense must be viewed as a defensive warfare activity.

Ensuring Security

To counter these threats, the DON will deploy an effective strategy (security architectures, policies, procedures and tactics) of aggressive active computer network defense within the NMCI structure. Although the DON intends to pursue an aggressive outsourcing strategy for the design, deployment and operation of the NMCI, it is important to note that only authorized Department of Defense (DoD) personnel will perform critical security roles. These security roles include ensuring that the NMCI satisfies DoD, DON, and Federal information security requirements, and exercising essential command authority over DON defense warfare activities.

The vendor is required to implement this security guidance and configurations in the NMCI architecture and seat configurations. In concert with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) the NMCI will meet fundamental security requirements, and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive but unclassified data. Further, DON personnel shall be the approving authority for the NMCI security architecture, security-critical product selections and security procedures as well as other security factors as required. DoD/DON blue teams will conduct design, product and configuration reviews. Simulated attacks by red teams against operational NMCI networks will help ensure that the NMCI satisfies related service level agreements (SLAs) and DoD/DON security requirements. When necessary, the DON will enlist the assistance of the Defense Information Systems Agency (DISA) and the National Security Agency (NSA) for red teaming efforts.

Defense in Depth

While perfect security in an information-sharing environment is nearly impossible, the NMCI will do much to minimize system vulnerabilities and counter potential threats. To this end, the DON has defined a Defense in Depth strategy that uses currently available protection technology, installed in a layered system of defenses - much the same way a bank vault may be built with sequential doors and many alarm systems. Defense in Depth is designed to protect the confidentially, integrity, authenticity and availability of the information and the systems in the NMCI environment. Protection methodologies and tools such as firewalls, packet filtering, intrusion detection systems, content filtering, virtual private network (VPN) architectures, Public Key Infrastructure (PKI) enabled applications, and large key encryption algorithms are the backbone of this initiative. While no single tool provides complete security, a well-planned deployment of multiple tools that complement and reinforce each other will significantly strengthen and harden the infrastructure.

For further information, please contact:

Program Executive Office Information Technology (PEO-IT)
2451 Crystal Drive, Suite 1109
Arlington, VA 22202-4804

PEO-IT Public Affairs Office (PAO)
703-602-3580
www.peo-it.navy.mil

For technical information, please contact:
Mr. Steven Ehrler
PEOIT-B
703-602-5026
ehrlers@spawar.navy.mil